EUROPEAN PATENT

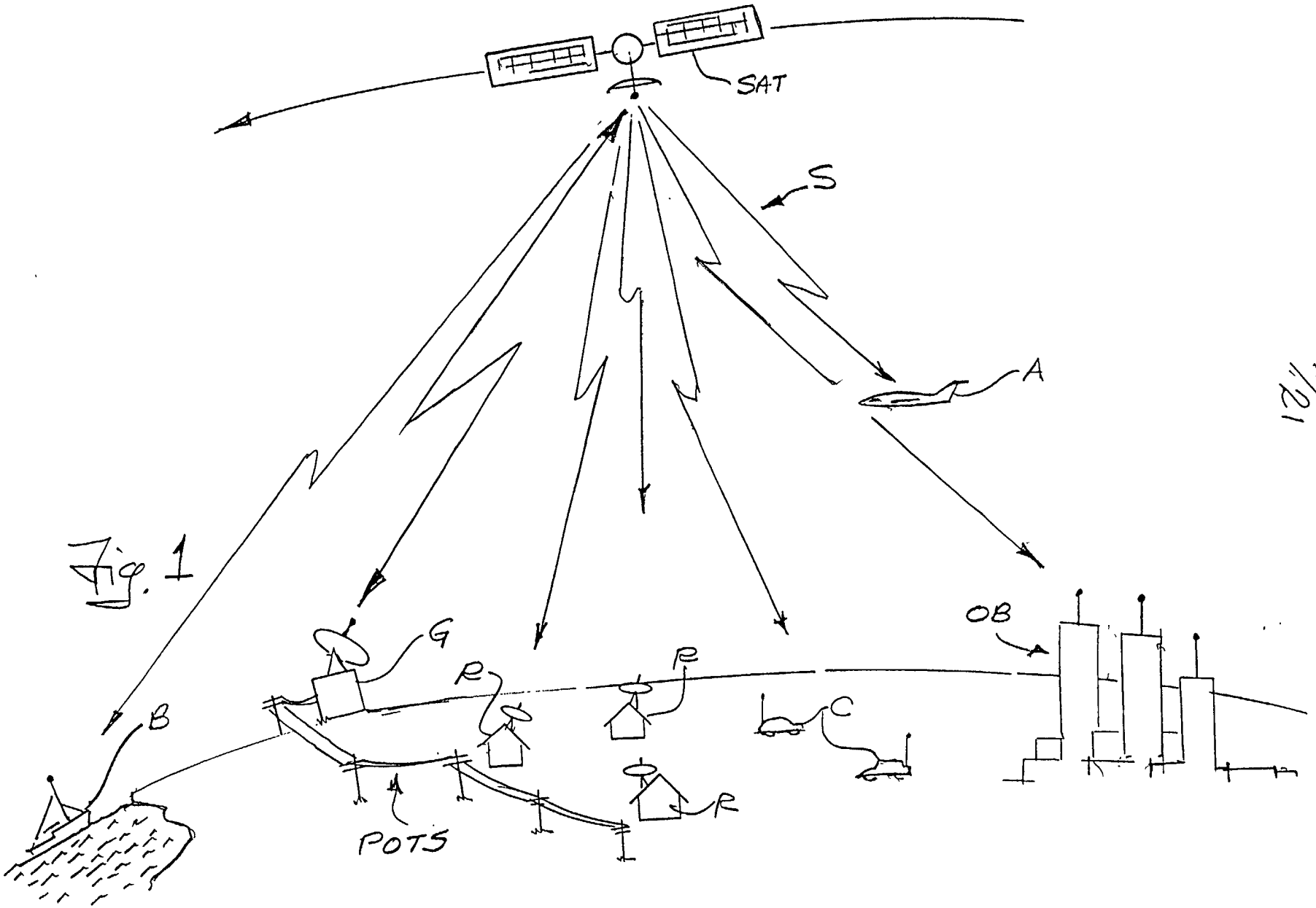


Fig. 1

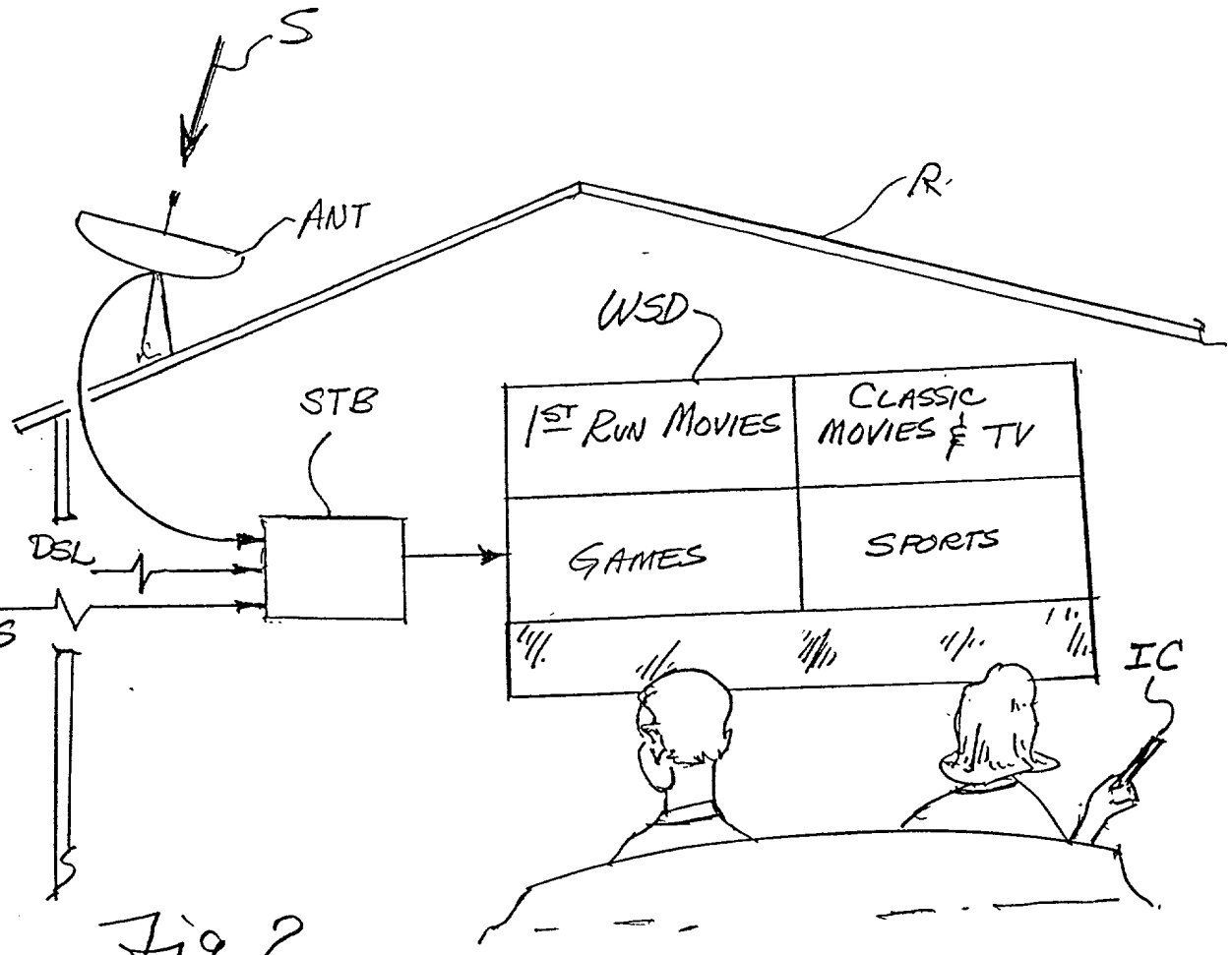

S
ANT
R
WSD
STB
1ST RUN MOVIES
CLASSIC MOVIES & TV
GAMES
SPORTS
DSL
POTS
IC

Fig. 2

Sky Vault Operation Flow Chart

Customer

↓

Customer Requests Program Material

↓

POTS, Internet, or Other Communication Medium

↓

System or System-licensed Program Material
Processing Center
-Material Verified
-Material Server or Storage Site Located
-Program "Free" Verified and Charged to Customer
Except on Fixed Monthly Account

↓

Program Material or Source Site
-Requested. Material Located and Prepared for Transmission
-Requested Material Sent Via Selected Network Path

↓

System or System Licensed Network

↓

Customer's Set-Top Box/Storage Sustem

↓

Customer Viewing as Desired

Fig. 2A

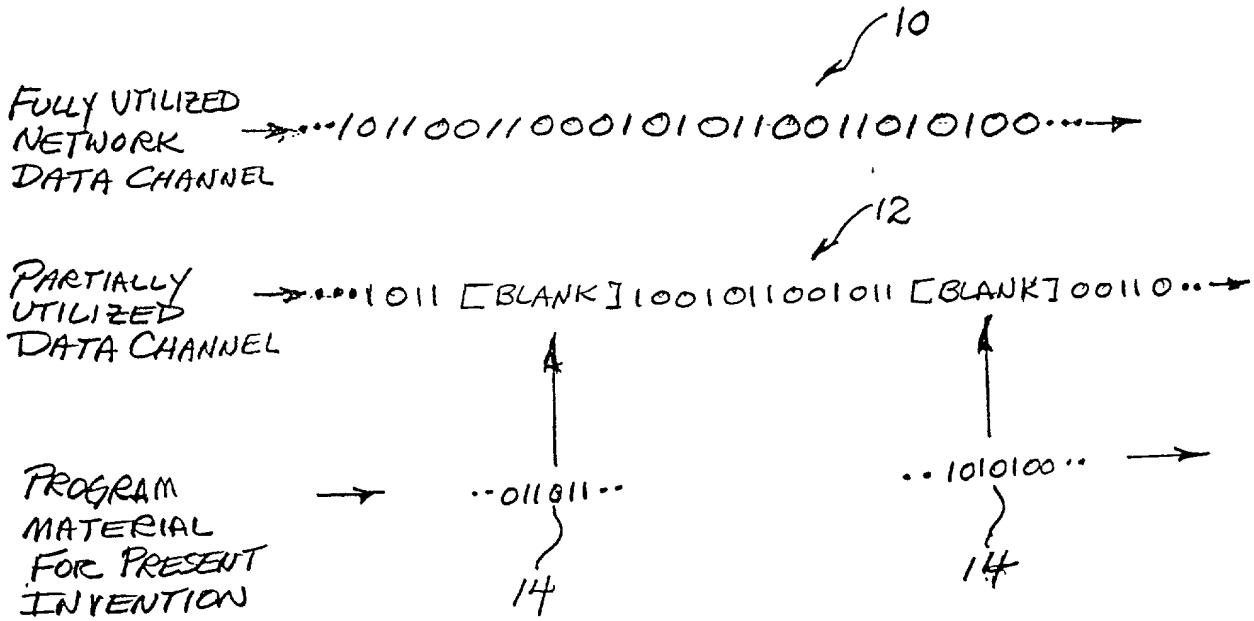

10
FULLY UTILIZED NETWORK DATA CHANNEL
...10110011000101011001101010 0...
12
PARTIALLY UTILIZED DATA CHANNEL
...1011 [BLANK] 1001011001011 [BLANK] 00110...
PROGRAM MATERIAL FOR PRESENT INVENTION
..011011..
14
..1010100..
14

Fig. 3

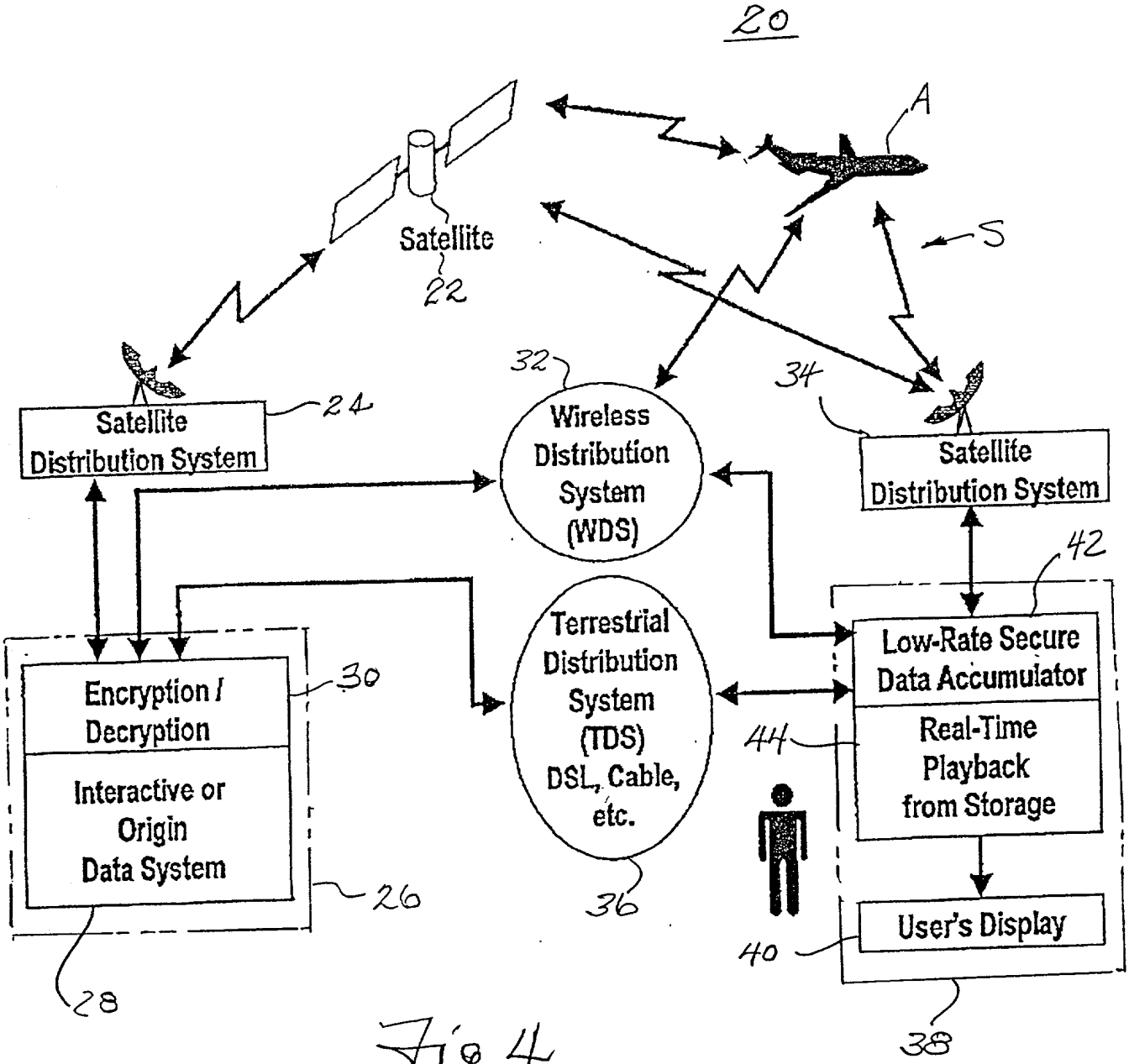

20
A
Satellite
22
S
32
34
Satellite
Distribution System
24
Wireless
Distribution
System
(WDS)
Satellite
Distribution System
42
Encryption /
Decryption
30
Interactive or
Origin
Data System
26
28
Terrestrial
Distribution
System
(TDS)
DSL, Cable,
etc.
36
Low-Rate Secure
Data Accumulator
44
Real-Time
Playback
from Storage
User's Display
40
38

Fig. 4

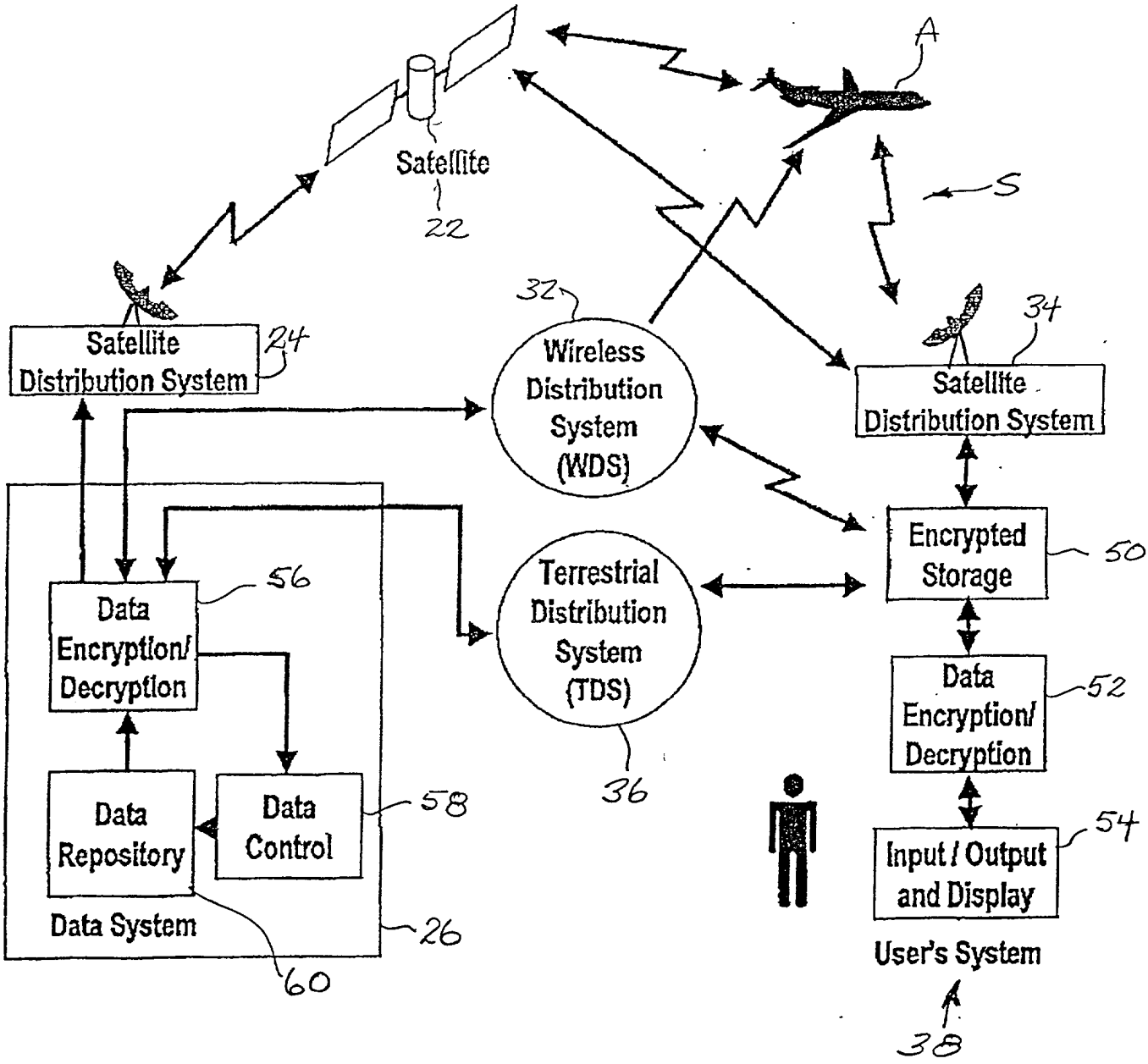

Satellite
22
A
S
Satellite Distribution System
24
32
Wireless Distribution System (WDS)
34
Satellite Distribution System
Encrypted Storage
50
Terrestrial Distribution System (TDS)
36
Data Encryption/ Decryption
56
Data Encryption/ Decryption
52
Data Repository
Data Control
58
Input / Output and Display
54
Data System
26
60
User's System
38

Fig. 5

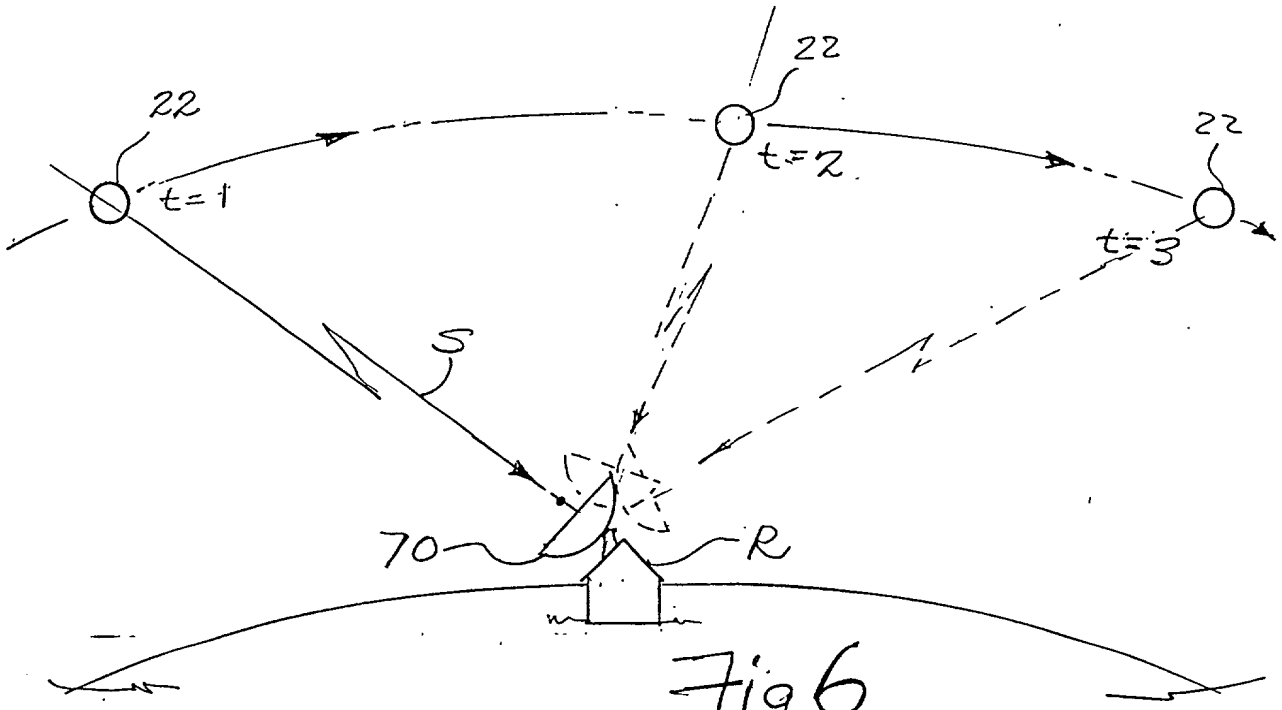


Fig. 6

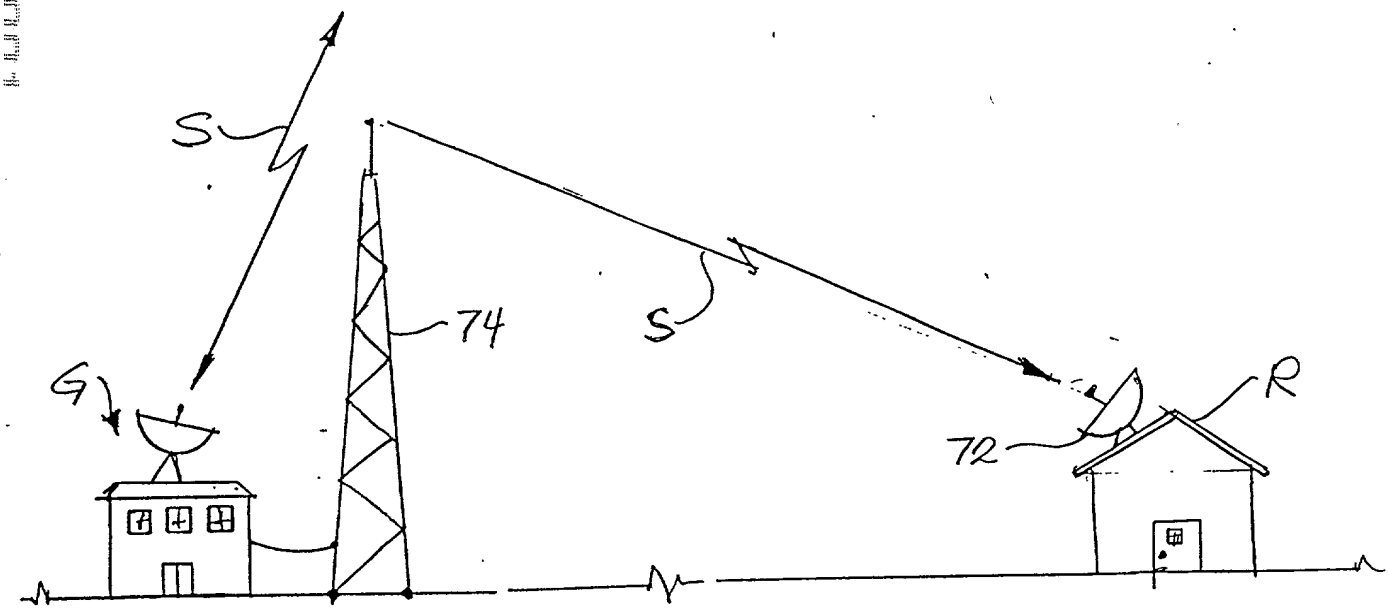


Fig. 7

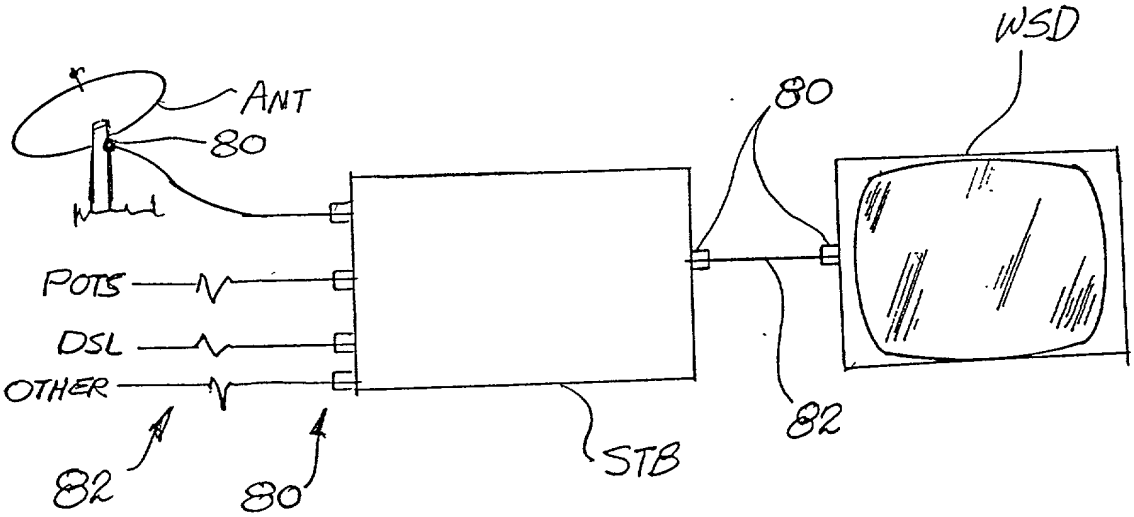

WSD
ANT
80
80
POTS
DSL
OTHER
82
80
STB
82

Fig. 8

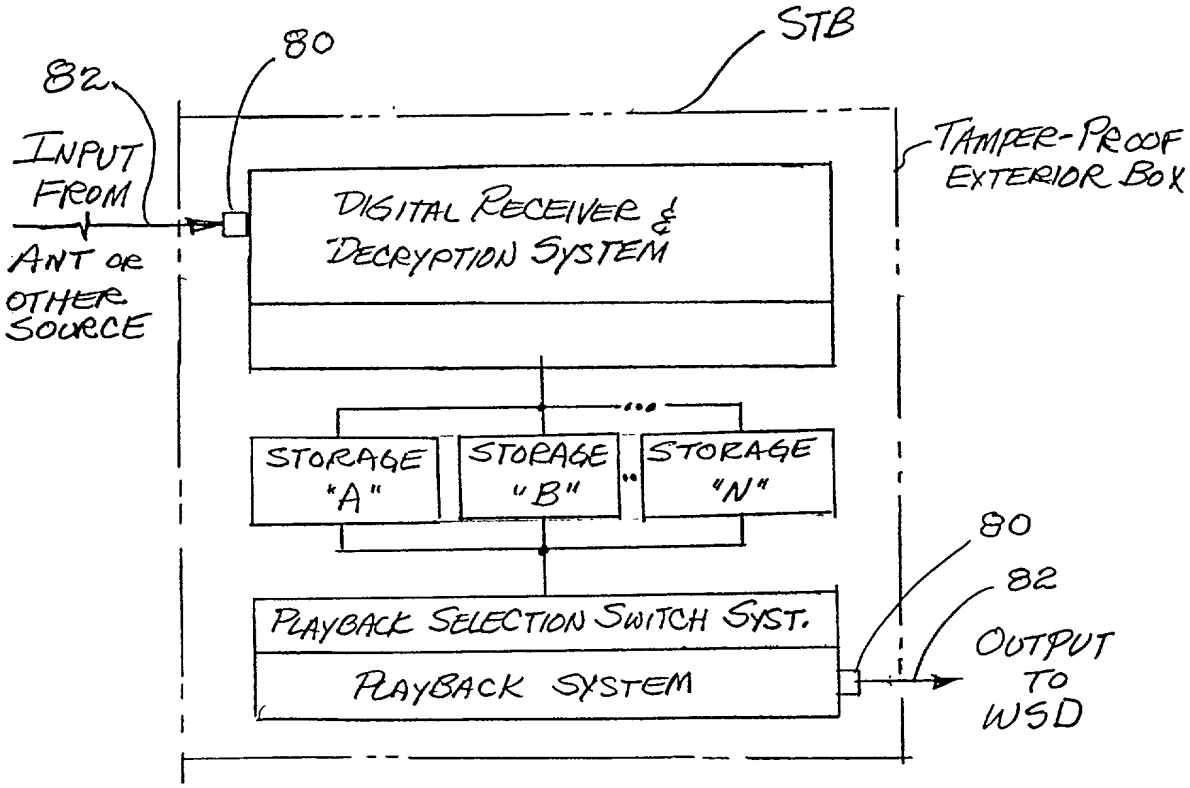

STB
82
80
INPUT FROM ANT OR OTHER SOURCE
TAMPER-PROOF EXTERIOR BOX
DIGITAL RECEIVER & DECRYPTION SYSTEM
STORAGE "A"
STORAGE "B"
STORAGE "N"
80
82
PLAYBACK SELECTION SWITCH SYST.
PLAYBACK SYSTEM
OUTPUT TO WSD

Fig 9

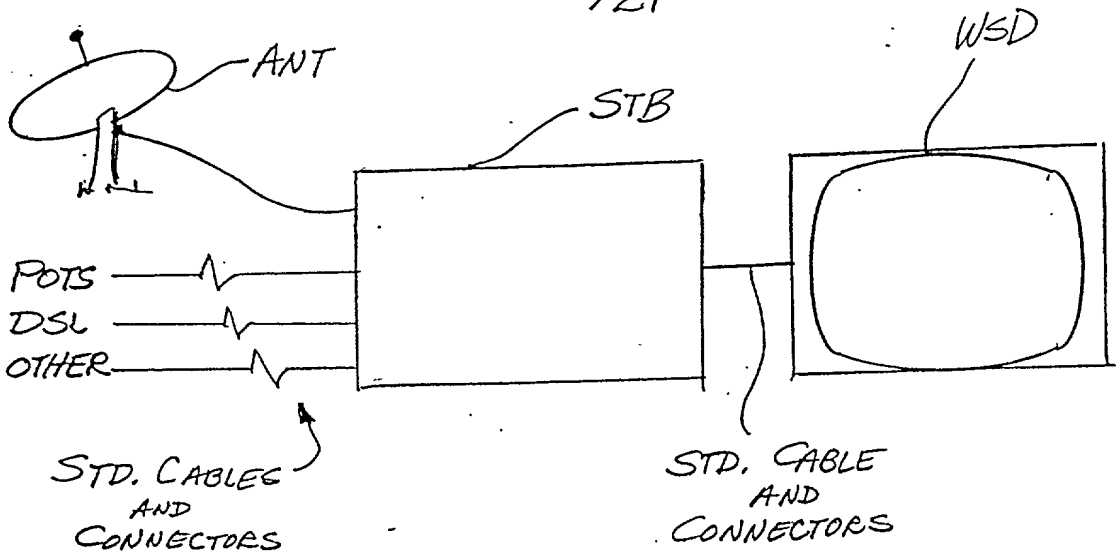

ANT
STB
WSD
POTS
DSL
OTHER
STD. CABLES AND CONNECTORS
STD. CABLE AND CONNECTORS

Fig 10

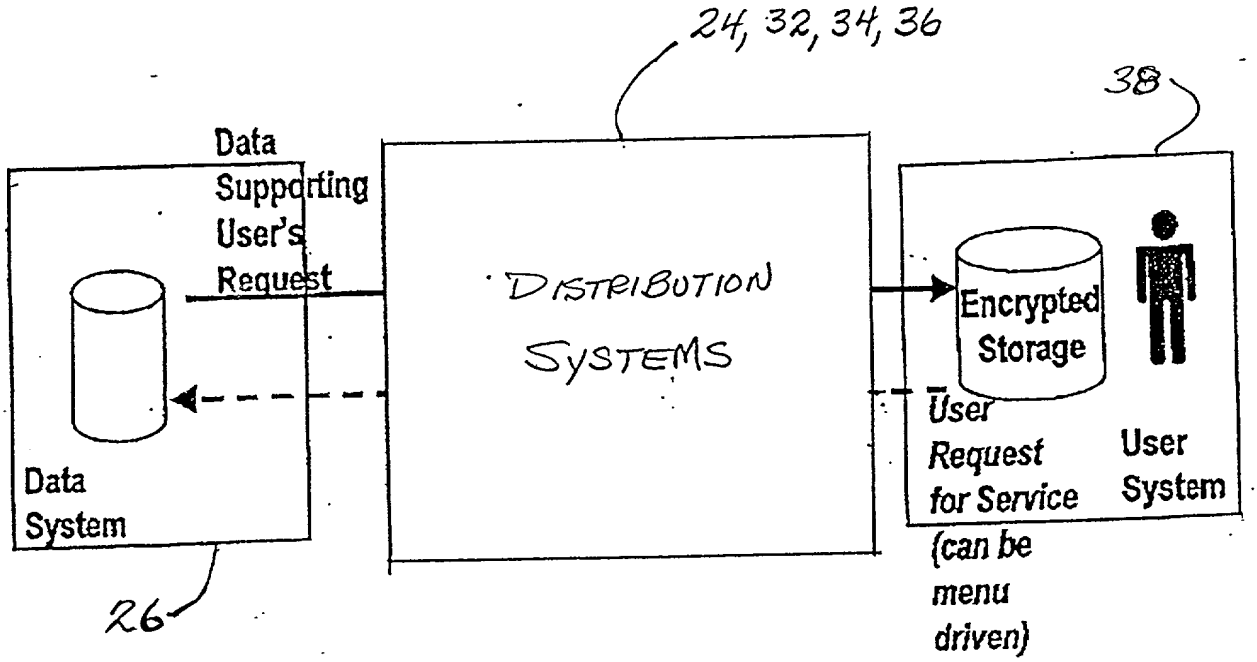

24, 32, 34, 36
38
Data Supporting User's Request
DISTRIBUTION SYSTEMS
Encrypted Storage
Data System
User Request for Service (can be menu driven)
User System
26

Fig. 11

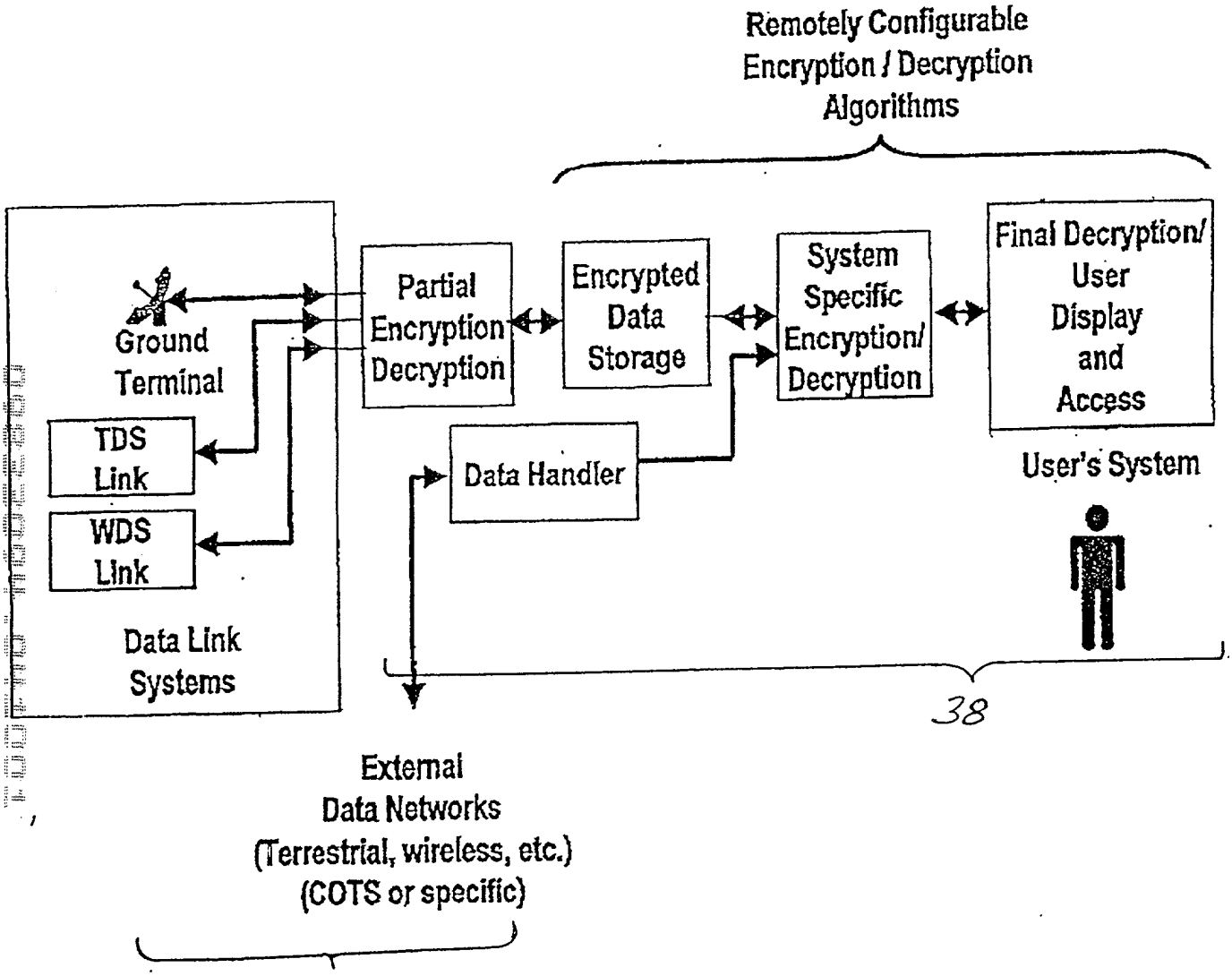

Remotely Configurable
Encryption / Decryption
Algorithms
Ground
Terminal
TDS
Link
WDS
Link
Data Link
Systems
Partial
Encryption
Decryption
Encrypted
Data
Storage
System
Specific
Encryption/
Decryption
Final Decryption/
User
Display
and
Access
User's System
Data Handler
38
External
Data Networks
(Terrestrial, wireless, etc.)
(COTS or specific)
24, 32, 34, 36

Fig 12

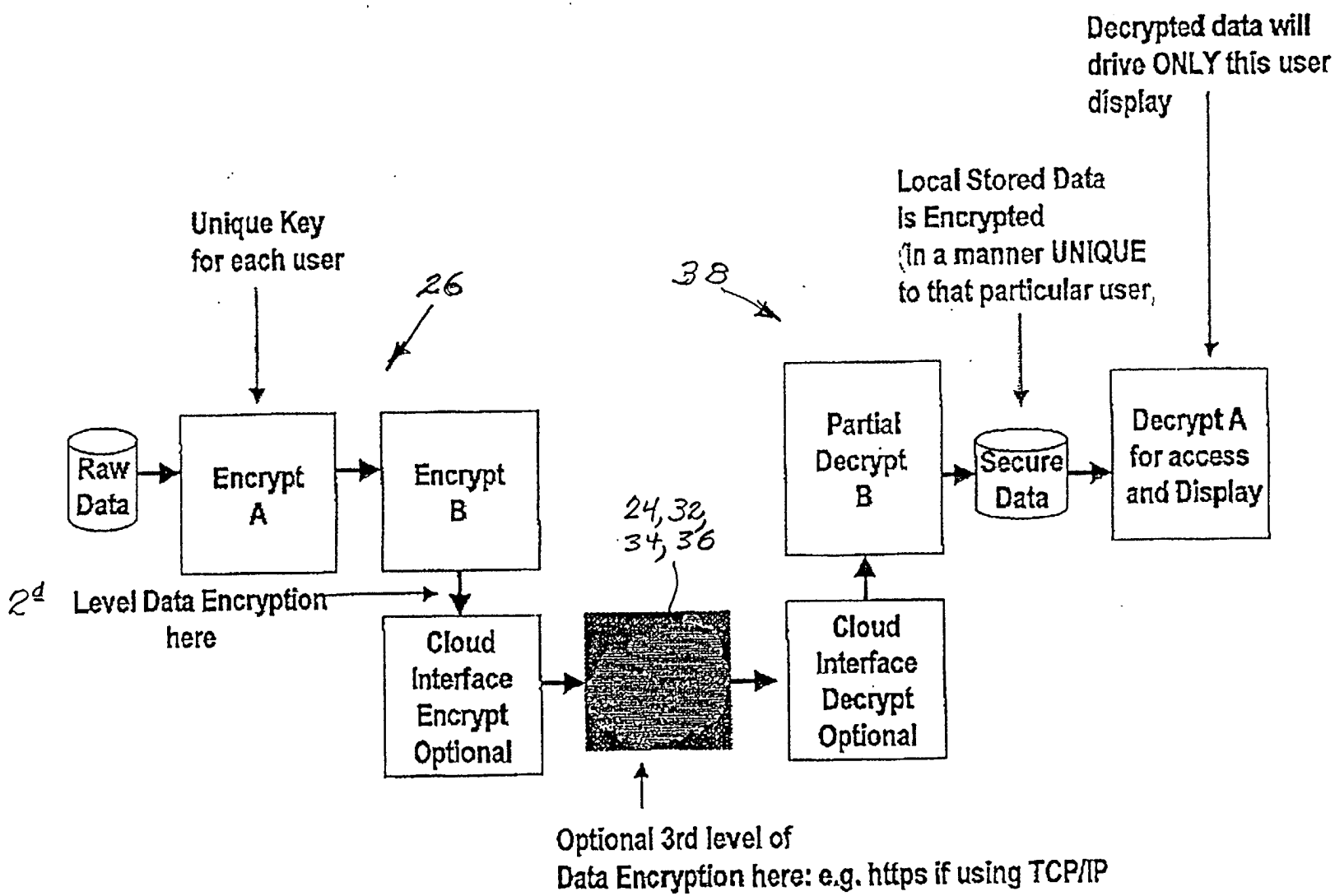

Decrypted data will drive ONLY this user display
Local Stored Data Is Encrypted (In a manner UNIQUE to that particular user,
Unique Key for each user
26
38
Raw Data
Encrypt A
Encrypt B
Partial Decrypt B
Secure Data
Decrypt A for access and Display
24, 32, 34, 36
2d Level Data Encryption here
Cloud Interface Encrypt Optional
Cloud Interface Decrypt Optional
Optional 3rd level of Data Encryption here: e.g. https if using TCP/IP

Fig. 13

12/21

SYSTEM SERVER FUNCTIONS

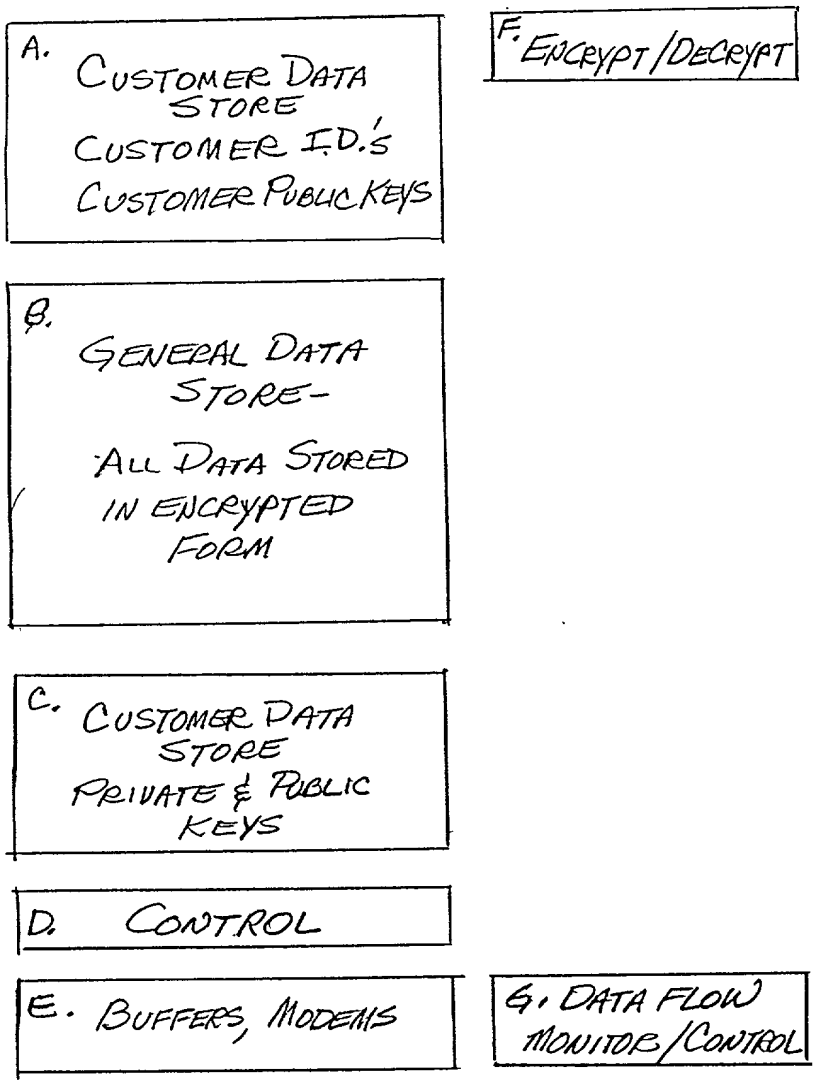
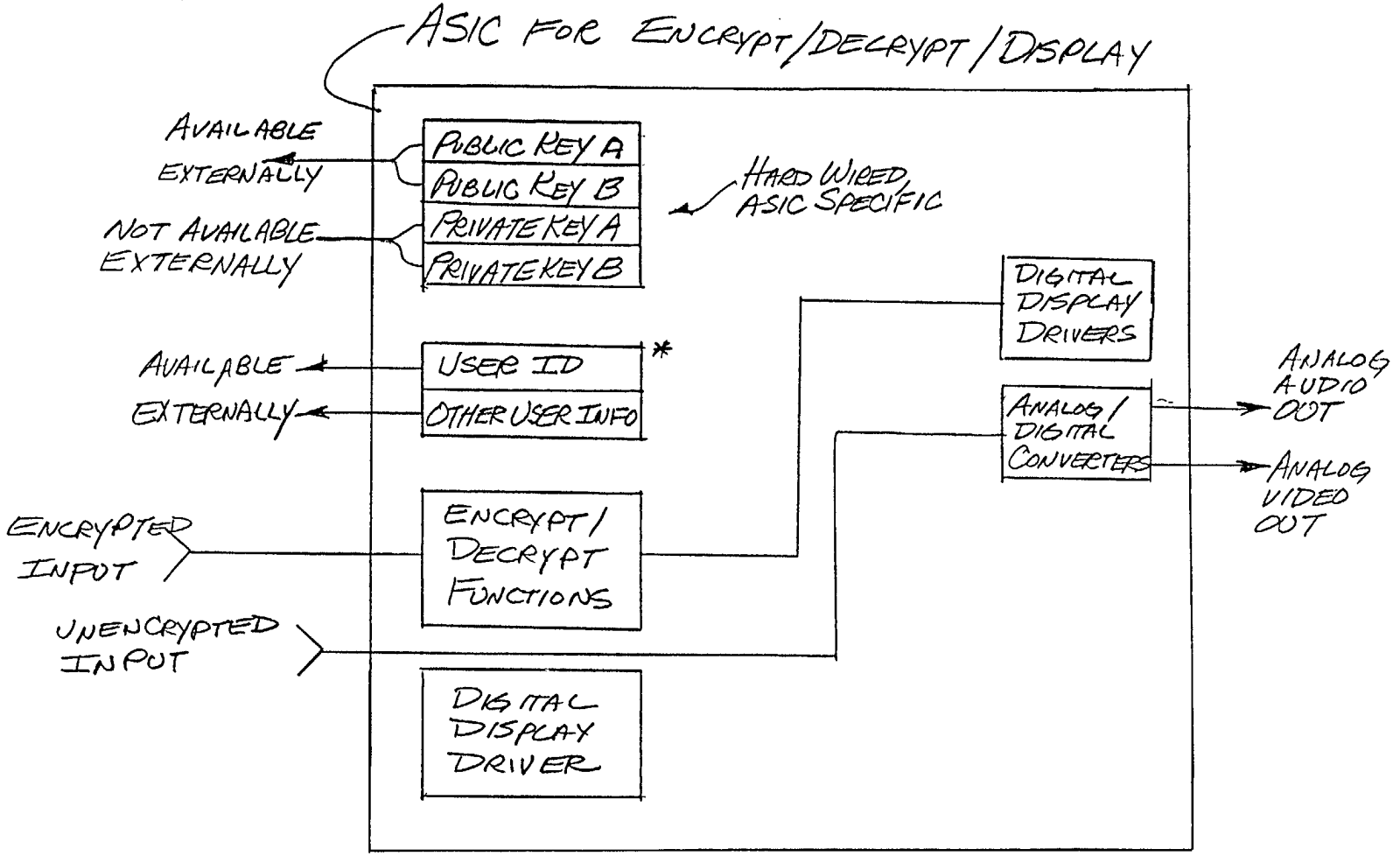


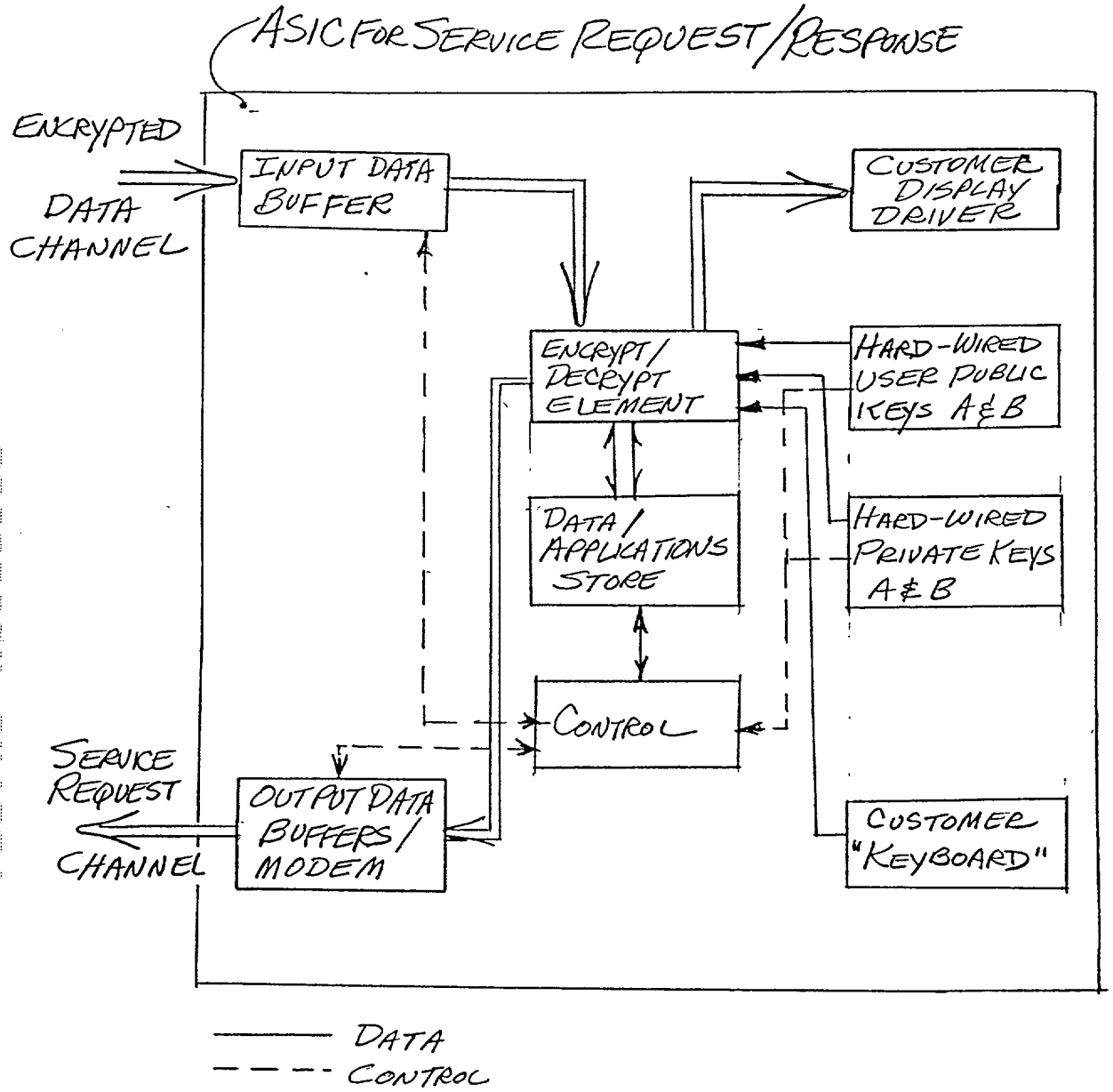
Fig. 14



* MAY BE STORED EXTERNALLY

NOTES: 1) CUSTOMER-SPECIFIC ASIC, ANALOG & DIGITAL CIRCUITS
2) NO DIGITAL, DECRYPTED DATA AVAILBLE EXTERNAL TO ASIC

Fig. 15



NOTES: 1) Request for data – CONTROL sends PUBLIC KEYS A&B to SYSTEM SOURCES via OUTPUT DATA BUFFER; sends DATA I.D. NUMBER to identify stored data upon receipt.

2) Data reception – CONTROL identifies DATA & applies Private Keys A or B for Storage or Display.

Fig. 16

Multiple Path "Rainbarrel" Data Delivery

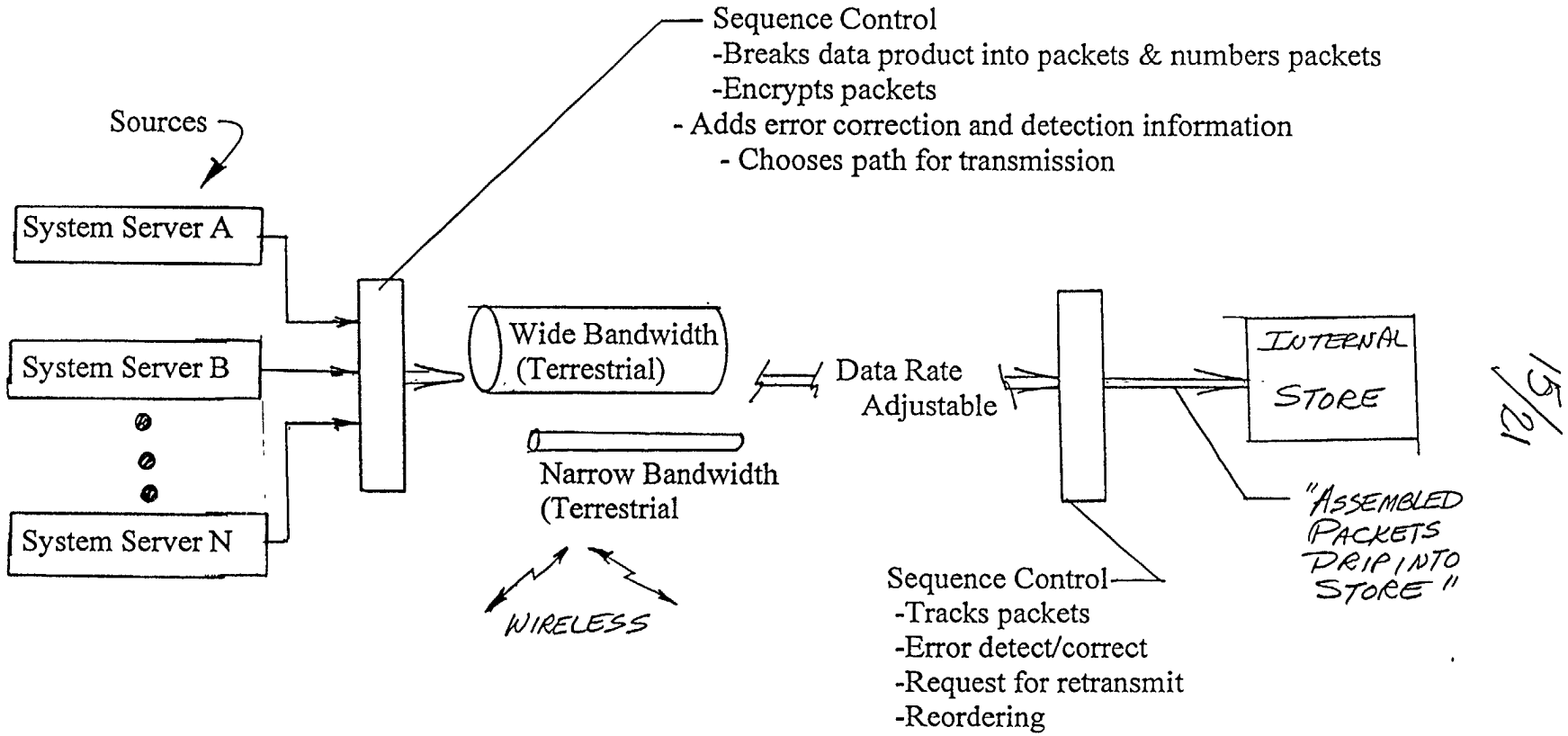


Fig.17

Request for Data and Response

1) Customer requests data menu from system server.

2) System server responds with menu, etc.

3) Customer requests "data".
- Generic request: customer sends customer ID, public key A; encrypts by public key.
- Request for specific data: customer sends ID, public keys A and B; encrypts by public key

4) Network encrypts/decrypts (for example, with https); system server decrypts and searches data base for response.

5) System server extracts data, "packetizes" the data.
-Server encrypts the data with public key A
-Network encrypts/decrypts

6) Network operating system routes encrypted packets over available routes to customer.

7) Customer decrypts with private key A
-Generic request: Display menu
-Specific request: Data buffered, reassembled and stored in encrypted form.

Fig. 18

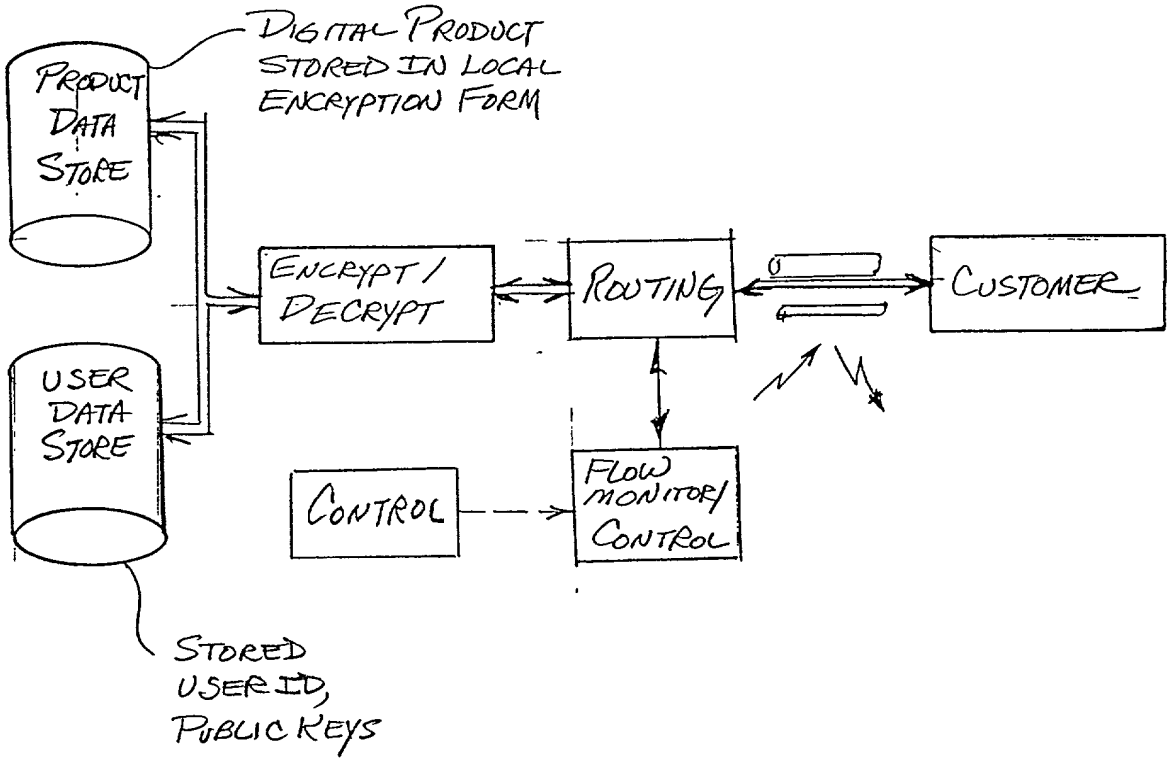
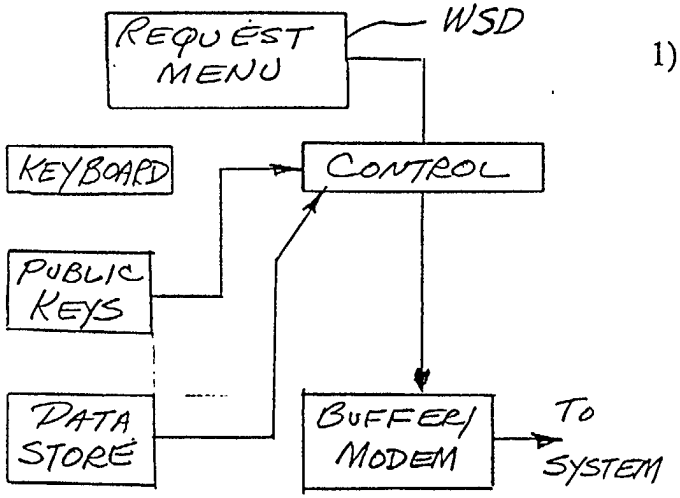

DIGITAL PRODUCT STORED IN LOCAL ENCRYPTION FORM
PRODUCT DATA STORE
USER DATA STORE
ENCRYPT / DECRYPT
ROUTING
CUSTOMER
CONTROL
FLOW MONITOR/ CONTROL
STORED USER ID, PUBLIC KEYS

Fig. 19

User Request for System Menu



1) At request for system menu, the following actions occur:
   - -Control extracts user ID, public keys A&B from user hardware
   - -Control extracts software application containing data request protocols from Data Store and directs request to Output Data Buffer/Modem.
   - -Encrypted request is transmitted to a system server via available channel.

   - -Additional encryption is available using https when using TCP/IP protocols over the channel.

12/91

2) At receipt of menu data, Control decrypts with private key B and stores in Data/Application Store.
3) When data transfer is complete, Control causes display to indicate "Menu Available."
4) Customer requests menu display from the keyboard (or mouse, etc.)
5) Control extracts encrypted data from Store and performs second decryption using private key A.
6) Data is displayed on screen, but digital unencrypted form of the data is unavailable outside of display ASIC.

Fig. 20

User Request for System Data

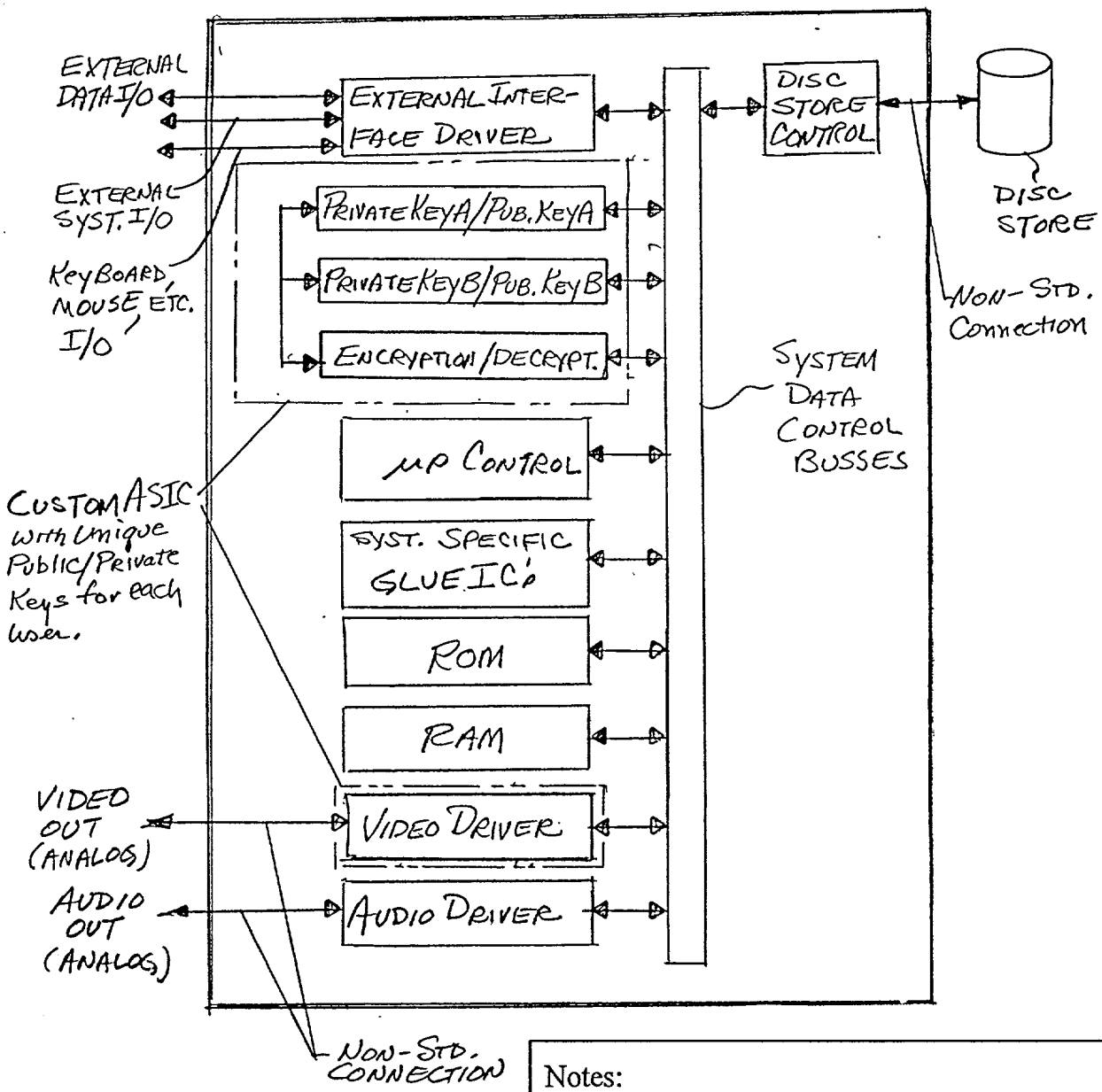
1) Customer requests system menu data by keyboard (or mouse, etc.)
2) Request is encrypted using public key A and stored in Data/Applications Store. Customer ID,, public keys A and B are attached.

3) Request is also encrypted using System public key and sent to Data Flow Monitor/Control and Buffers/modems for transmission via available digital channel.

4) At receipt of data request by System, the following actions occur:
-Controller stores customer request in a General Data Store.
-Requested data is encrypted using customer public keys A & B and sent to data Flow Monitor/Control for progressive transmission through buffers/modems.
-Selected least significant bits of data, controlled by customer poublic key, are altered with a **customer-specific** signature.
5) When customer receives data, Control decrypts data using private key B and stores data blocks in Data/Applications Store. When all data blocks are received, Control notifies user via the display.
6) When customer requests to view the data, Control decrypts it using private key A and removes the digital signature. Control then sends the data to the display driver.
7) Note that all keys are hardware specific and not available to the operating system. They are usable only by the encrypt/decrypt/display ASIC. No "Hacker" access since digital data is never available outside the user's hardware.

12/61

Fig. 21



Notes:
1. Public keys available on System Data Bus.
2. Private keys within and only available to encryption/decryption ASIC.
3. Digital data never available outside of ASIC in unencrypted form.
4. All data stored on disc, or equivalent, is in encrypted form.
5. Analog video and audio data transmitted to off-board displays via non-standard connectors and cables.

Fig. 22

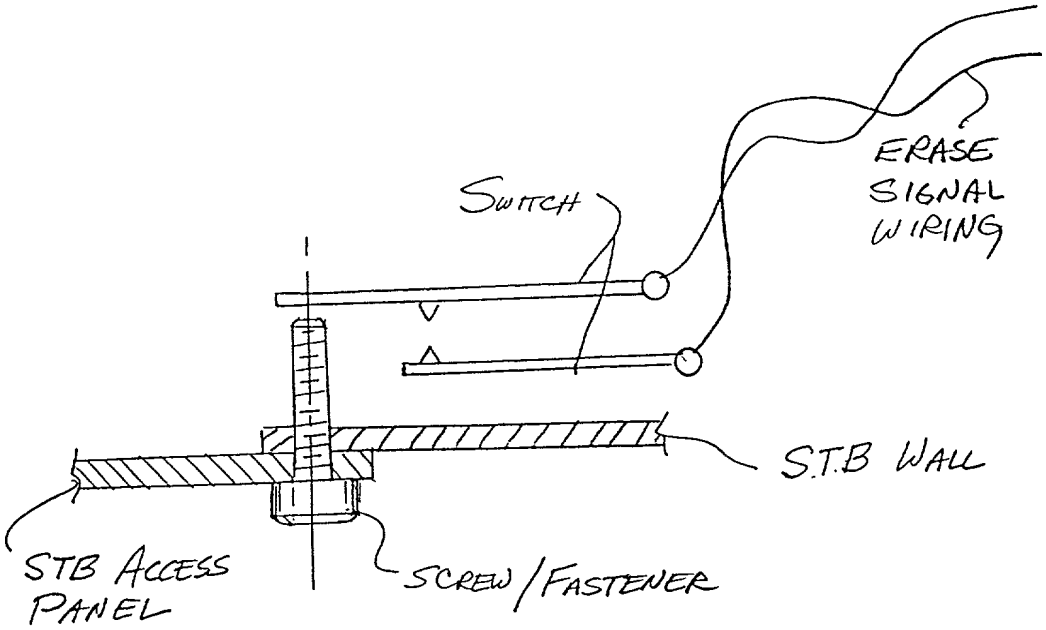

ERASE
SIGNAL
WIRING
SWITCH
S.T.B WALL
STB ACCESS
PANEL
SCREW/FASTENER

Fig. 23